

UNCLASSIFIED



NORTH DAKOTA HOMELAND SECURITY ANTI-TERRORISM SUMMARY



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

UNCLASSIFIED

NDSLIC DISCLAIMER

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

[North Dakota](#)

[Regional](#)

[National](#)

[International](#)

[Banking and Finance Industry](#)

[Chemical and Hazardous Materials
Sector](#)

[Commercial Facilities](#)

[Communications Sector](#)

[Critical Manufacturing](#)

[Defense Industrial Base Sector](#)

[Emergency Services](#)

[Energy](#)

[Food and Agriculture](#)

[Government Sector \(including
Schools and Universities\)](#)

[Information Technology and
Telecommunications](#)

[National Monuments and Icons](#)

[Postal and Shipping](#)

[Public Health](#)

[Transportation](#)

[Water and Dams](#)

[North Dakota Homeland Security
Contacts](#)

UNCLASSIFIED

NORTH DAKOTA

Nothing Significant to Report

REGIONAL

(South Dakota) SD college student pleads guilty to making threats. A South Dakota college student accused of threatening to shoot people on campus and burn down a dean's house said he never intended to harm anyone. He appeared in court July 30 and pleaded guilty to making a terroristic threat at the South Dakota School of Mines and Technology. Under terms of the plea agreement, prosecutors recommended local jail time and probation, along with a psychological evaluation. The decision on punishment rests with the judge, who could impose up to 5 years in prison and a \$10,000 fine. Authorities said the student left a letter at the student union April 17 containing the threats and that he signed it BTK, the signature of a Kansas serial killer. Source: <http://www.sfgate.com/news/article/SD-college-student-pleads-guilty-to-making-threats-3749735.php>

NATIONAL

Cybersecurity bill fails to advance in Senate. August 2, after months of wrangling, the U.S. Senate rejected calls by the Presidential Administration and failed to advance sweeping legislation aimed at protecting American computer networks from cyberattacks. The cloture vote to end debate on the bill was 52-46, with 60 votes needed to advance the measure. The White House and top national security and defense leaders pressed the Senate to pass the Cybersecurity Act of 2012, but negotiations between Democratic supporters and Republican critics failed to yield an agreement. Republicans in the Senate echoed industry concerns that the bill could lead to government regulation, but debate over the legislation devolved into assigning blame. Source: <http://www.nextgov.com/cybersecurity/2012/08/cybersecurity-bill-fails-advance-senate/57185/>

INTERNATIONAL

Chevron, Transocean must stop drilling after spill in Brazil. A federal court gave Chevron and driller Transocean 30 days to suspend all petroleum drilling and transportation operations in Brazil until investigations are completed on two oil spills off the coast of Rio de Janeiro. The court said in a statement posted August 1 on its Web site that each company will be fined \$244 million for each day they fail to comply with the suspension. About 155,000 gallons of oil crude began seeping from cracks in the ocean floor at the site of a Chevron appraisal well in November 2011. Chevron placed the amount of oil that leaked at 110,000 gallons. Two weeks later, the National Petroleum Agency said the seepage was under control. However, in March, oil again started leaking and Chevron voluntarily suspended production in the field. The head of Brazil's petroleum agency said the November spill involved about 25 safety infractions for which Chevron will be fined up about \$25 million, the maximum under Brazilian law. Chevron said it underestimated the pressure in an underwater reservoir, causing crude to rush up a bore

UNCLASSIFIED

hole and escape into the surrounding seabed about 230 miles off Rio de Janeiro. The oil seeped from at least seven narrow fissures on the ocean floor, all within 160 feet of the wellhead. No oil reached shore. Source: <http://www.usatoday.com/money/industries/energy/story/2012-08-01/chevron-brazil-oil-spill-transocean/56657294/1>

Bomb scare closes US Embassy in Norway. The U.S. Embassy and an area of central Oslo, Norway, were evacuated July 31 when a fake explosive device was mistakenly left beneath a vehicle trying to enter the compound, police said. The discovery of the device by security guards also led to the evacuation of the royal palace, the halting of subway traffic in the area, and the cancellation of an international children's soccer game at nearby Voldslokka Stadium so police could use the field for helicopters. The bomb scare and police search closed the entire area for several hours. "The Oslo police bomb squad has removed the object and can confirm that it was a dummy bomb," police said in a statement. "The car has been used for an internal drill at the embassy, and the find can be connected to this." Source: <http://www.npr.org/templates/story/story.php?storyId=157637141>

Canada kicks off genome mapping of Listeria. Canada kicked off a \$600,000 project to map the genome of Listeria bacteria so that more rapid tests can be developed, Food Safety News reported July 31. The Canadian Food Inspection Agency (CFIA), Genome Canada, and Alberta Innovates Bio Solutions are teaming up to help protect consumers from the food-borne illness. The 18-month research initiative is being funded with \$250,000 each from Genome Canada and CFIA, and \$100,000 from Alberta Innovates Bio Solutions. Currently, it takes at least 5 days to confirm the presence of Listeria. Genomic mapping could improve accuracy and cut the time it takes for both the government and industry to identify Listeria contamination. Source: <http://www.foodsafetynews.com/2012/07/canada-kicks-off-genome-mapping-of-listeria/>

BANKING AND FINANCE INDUSTRY

IRS missing billions in ID theft. The Internal Revenue Service (IRS) may have delivered more than \$5 billion in refund checks to identity thieves who filed fraudulent tax returns for 2011, Treasury Department investigators said August 2. They estimated another \$21 billion could make its way to ID thieves' pockets over the next 5 years. The IRS detected far fewer fraudulent tax refund claims than actually occur, a government audit stated. Although the IRS detected about 940,000 fraudulent returns for 2011 claiming \$6.5 billion in refunds, there were potentially another 1.5 million undetected cases of thieves seeking refunds after assuming the identity of a dead person, child, or someone else who normally would not file a tax return. Topping the list of concerns was the IRS's lack of timely access to third-party information it needs to verify returns and root out fraud. Due to the gap between when taxpayers can start filing returns and when employers and financial institutions are required to submit withholding and income documents to taxpayers, the IRS often issues refunds before it can confirm the information on the returns. Of the 1.5 million undetected cases of potential fraud, 1.2 million used direct deposits. Source: <http://www.boston.com/business/personal-finance/taxes/2012/08/02/irs-missing-billions-theft/vHJriJPNyuc1NuTANdzLHL/story.html>

UNCLASSIFIED

UNCLASSIFIED

Error by Knight Capital rips through stock market. A technology breakdown at a major trading firm roiled the prices of 140 stocks listed on the New York Stock Exchange August 1. The problems at Knight Capital Group Inc, one of the largest firms that buys and sells stocks to provide liquidity to the markets, emerged at the beginning of trading. Heavy computer-based trading caused a rush of orders for dozens of stocks, whose shares soared far beyond their previous day closing prices. The trading glitches were the latest in a series of market snafus that have hurt retail investors' confidence, including the botched Facebook initial public offering, the 2010 "flash crash" in which nearly \$1 trillion in market value disappeared in minutes, and the failed public offering of BATS Global Markets. The exact nature of the technology issues was unclear. Source: <http://www.reuters.com/article/2012/08/01/us-usa-nyse-tradinghalts-idUSBRE8701BN20120801>

2 poker sites agree to forfeit \$731 million after prosecutors allege 'global Ponzi scheme'. The world's largest poker company and its rival have settled federal money laundering and fraud charges, agreeing to pay \$731 million, most of which will be used to reimburse online gamblers, NBC News reported August 1. PokerStars, which is based on the Isle of Man in the United Kingdom, agreed to forfeit the money, including \$547 million that will be available to reimburse U.S. customers of the rival, Full Tilt Poker. Full Tilt also agreed to settle and will cease independent operations. Prosecutors said both companies had used false billing codes to deceive banks that would not process gambling transactions, and they said Full Tilt had devolved into a "global Ponzi scheme," with the big-name players and other owners pocketing hundreds of millions of dollars that were owed to players. Prosecutors accused Full Tilt of lying when it told customers that their accounts were "segregated and held separately" from the company's operating funds. In the end, it owed more than it could repay without a sale. Source: http://www.msnbc.msn.com/id/48433962/ns/us_news-crime_and_courts/#.UBIB3GGe6NA

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Nuclear smuggling shows terrorist WMD threat persists: State Department. The U.S. Department of State July 31 said that the attempted smuggling of nuclear arms-grade uranium in recent years illustrates a continued risk that terrorists could acquire the ingredients for a weapon of mass destruction. The department's Country Reports on Terrorism 2011 touted as "largely successful" multilateral programs aimed at locking down chemical, biological, radiological, and nuclear materials around the globe. However, "the illicit trafficking of these materials persists, including instances involving highly enriched uranium in 2010 and 2011," the report stated. Source: <http://www.nti.org/gsn/article/state-report/>

COMMERCIAL FACILITIES

(Pennsylvania) Market Square reopens after Pittsburgh bomb squad detonates suitcase. Pittsburgh police reopened Market Square after the bomb squad detonated a suspicious package there August 3. Police evacuated the square and roped it off. A police officer at Market Square said the bosquad found a suitcase that may have had a wire sticking out. A member of the bosquad in a protective suit put a plate on the suitcase to X-ray it, then returned to

UNCLASSIFIED

UNCLASSIFIED

thesquad's truck to view the images. Later, the bomb squad detonated the suitcase with a small, controlled explosion and planned to examine its contents. Source: <http://old.post-gazette.com/pg/12216/1251375-53.stm>

(Wisconsin) 2 die in shooting at northwest side manufacturing plant. A shooting inside a Trans-Coil International (TCI) manufacturing plant in Milwaukee left two men dead August 2, police said. A supervisor was shot multiple times by an employee who then shot himself. A handgun was recovered at the scene. WISN 12 Milwaukee reported that third-shift workers arriving at TCI were told the plant was closed for the night and would remain closed August 3. Source: <http://www.jsonline.com/news/milwaukee/2-die-in-shooting-at-northwest-side-manufacturing-plant-9u6bqk7-164836596.html>

COMMUNICATIONS SECTOR

Glitch in the nation's new weather alert system. The nation's new weather alert system experienced an error August 2. The frightening —Severe alert! Flash flood warning messages caught the attention of mobile-phone users across the Philadelphia region. The issue was that most of the people who received the warnings were in no danger whatsoever. Some of the areas warned were far removed from the areas endangered. August 2, flood warnings were issued for selected portions of Philadelphia, Bucks, Chester, and Montgomery Counties in Pennsylvania. Beamed from cell towers, however, the alerts they triggered lapped well beyond the targeted areas and into places unaffected by local weather. A standard free feature on many mobile devices sold approximately within the last year, the system began operation in April to carry alerts for assorted natural and unnatural disasters. The weather-alert piece came online in June. The alerts — for floods, tornadoes or hurricanes — are announced by special ringtones or vibrations. August 2, mobile users were told to —check local media. Source: http://articles.philly.com/2012-08-02/news/33001824_1_alert-system-flood-warnings-weather-alert

Massive phishing scam hits AT&T customers. Websense detected a massive phishing campaign targeting AT&T customers, sending in excess of 200,000 fake emails masquerading as billing information. The phishing emails, pretending to be from the American communication services provider, were discovered by Websense August 2. The fake emails look to scam consumers containing bogus claims that they owe AT&T hundreds of dollars. The email also reportedly houses a malicious link that lets the scam author's infect victims' machines. —Clicking on the link in the bogus message sends the user to a compromised web server that redirects the browser to a Blackhole exploit kit. As a result, malware is downloaded onto the computer that is currently not detected by most anti-virus products, according to VirusTotal, read Websense's blog. Source: <http://www.v3.co.uk/v3-uk/news/2196588/massive-phishing-scam-hits-at-t-customers>

Firm sees more DDoS attacks aimed at telecom systems. Attackers are now using distributed denial-of-service (DDoS) services that offer attacks on telecommunication systems as part of larger attack schemes. These attacks, known as TDoS attacks, can be a relatively cheap option

UNCLASSIFIED

UNCLASSIFIED

for cyber criminals seeking to diversify their attack vectors. Researchers have seen a series of advertisements and forum posts promoting services that can “flood” both mobile and stationary telephone lines. Often these attacks are used as a distraction while attackers launch simultaneous attacks on their victims, according to a member of Arbor Networks’ Security Engineering and Response Team. Source: http://threatpost.com/en_us/blogs/firm-sees-more-ddos-attacks-aimed-telecom-systems-073112

CRITICAL MANUFACTURING

Sears recalls Kenmore dehumidifiers due to fire and burn hazards. The U.S. Consumer Product Safety Commission, in cooperation with Sears and Kmart, August 2 announced a voluntary recall of about 795,000 Kenmore dehumidifiers. Consumers should stop using recalled products immediately unless otherwise instructed. The dehumidifiers can overheat, smoke, melt, and catch on fire, posing fire and burn hazards to consumers. Sears received 107 reports of incidents, with more than \$7 million in property damage and 3 reports of smoke inhalation injuries. The dehumidifiers were sold at Sears and Kmart stores nationwide and Sears.com and Kmart.com from 2003 to 2009. Source:

<http://www.cpsc.gov/cpscpub/prereel/prhtml12/12240.html>

Toyota recalling 760,000 RAV4’s due to crash risk. Toyota announced the recall August 1 of some 778,000 vehicles in the United States due to a suspension problem that could cause crashes. The recall comprises roughly 760,000 Toyota RAV4’s from model years 2006 to 2011, as well as about 18,000 Lexus HS 250h’s from 2010. Toyota said if the nuts on the rear suspension arms of these vehicles are not tightened properly during a wheel alignment service, the arms may come loose or separate. A Toyota spokesman said that so far in the United States, there have been “nine crashes and three minor injuries alleged to be related to this condition.” About 100,000 vehicles in Canada were also part of the recall. Source:

http://money.cnn.com/2012/08/01/autos/toyota-rav4-recall/index.htm?hpt=hp_t3

Hyundai recalls Santa Fe, Sonata on air bag issues. Hyundai Motor Co announced July 30 the recall of 199,118 Santa Fe sport utility vehicles (SUV) and 22,513 Sonata sedans in the U.S. for separate air bag issues. Santa Fe SUVs that were made from April 2006 through July 7, 2008, were recalled because the front passenger air bag may not deploy in a crash, the National Highway Traffic Safety Administration said. The airbag sensors may have difficulty detecting small adults seated in the front passenger seat. Separately, Hyundai is recalling Sonata sedans from the model years 2012-2013, made from January to June, because the side air bag may inflate unexpectedly, to the surprise of the driver. Source:

<http://www.reuters.com/article/2012/07/30/us-hyundai-recall-idUSBRE86TOPC20120730>

DEFENSE/ INDUSTRY BASE SECTOR

Nothing Significant to Report

UNCLASSIFIED

EMERGENCY SERVICES

(Texas) **Staffing shortage idle more prison beds.** Four additional dorms housing 320 convicts are being closed at a large maximum-security South Texas prison because of a continuing shortage of staff at the lockup, officials confirmed August 2. The move marks the largest such temporary closure of portions of a State prison in well over a decade, even during previous staffing stages that forced dorms at several prisons to be shut for many months. A spokesman for the Texas Department of Criminal Justice said the convicts will be transferred from the Connally Unit in Kenedy, about 55 miles southeast of San Antonio, to other State prisons in coming weeks. Source: http://www.statesman.com/blogs/content/shared-gen/blogs/austin/politics/entries/2012/08/02/staffing_shortage_idle_more_pr.html?cxntfid=blogs_postcards

(Vermont) **Vt. man crushes police cars with family tractor.** A man is accused of single-handedly leaving a path of destruction at one police station in Orleans County, Vermont. The suspect will be in Orleans County criminal court August 3, charged with crushing cars under a tractor. Police said the man took his family's farm tractor and ran over seven police cars in the Orleans County sheriff's department parking lot August 2. The suspect was allegedly seeking revenge after being arrested for resisting arrest after being caught with marijuana earlier. The man faces seven counts of unlawful mischief, as well as leaving the scene of an accident, among other charges. He is being held on \$15,000 bail. Source: <http://www.necn.com/08/03/12/Vt-man-crushes-police-cars-with-family-t/landing.html?blockID=750725&feedID=4753>

ENERGY

(Wisconsin) **U.S. regulator blocks restart of Enbridge Line 14.** The U.S. government blocked Enbridge from restarting a key Midwestern oil pipeline July 31, saying the spill the week of July 23 on the line was "absolutely unacceptable." The U.S. Transportation secretary blasted Enbridge over the leak of more than 1,000 barrels of crude oil in a field in Wisconsin, which shut down its 318,000 barrel per day pipeline July 27. "I will soon meet with Enbridge's leadership team, and they will need to demonstrate why they should be allowed to continue to operate this Wisconsin pipeline without either a significant overhaul or a complete replacement," the secretary said in a statement. Federal regulator Pipeline and Hazardous Materials Safety Administration (PHMSA) delivered a corrective order to Enbridge July 31, prohibiting it from restarting Line 14 until it can show regulators it has met safety standards. In a statement, Enbridge said it plans to complete repairs to Line 14 by August 1, and will submit plans to PHMSA to restart the line. The secretary said there was no guarantee that permission would be granted to restart the line anytime soon. Corrective orders can delay resumption of pipeline operations, sometimes for weeks or months. Source: <http://www.reuters.com/article/2012/07/31/us-enbridge-pipeline-regulator-idUSBRE86U1DK20120731>

(Wisconsin) **Wis. utility to spend \$430M to reduce emissions.** Alliant Energy said it would spend as much as \$430 million to reduce emissions at its coal-fired plant in Sheboygan,

UNCLASSIFIED

Wisconsin. The utility said July 27 it would install a system to reduce emissions of sulfur dioxide from the largest of its three coal-fired generators. The Sheboygan Press reported the project must first be approved by the State Public Service Commission. Alliant officials also plan to retire the oldest of the Edgewater Generating Station's three coal generators by 2015. They will also decide by 2013 whether to switch the other to natural gas or to shut it down. Source: <http://dailyreporter.com/2012/07/30/wis-utility-to-spend-430m-to-reduce-emissions/comment-page-1/>

FOOD AND AGRICULTURE

Small drought assistance and more disaster counties. The U.S. Agriculture Secretary announced two new pieces of disaster assistance for farmers and ranchers impacted by the nation's worsening drought, the U.S. Department of Agriculture (USDA) announced August 2. First, he is expanding emergency haying and grazing on approximately 3.8 million acres of conservation land to bring greater relief to livestock producers dealing with shortages of hay and pastureland. Second, the Secretary announced that crop insurance companies agreed to provide a short grace period for farmers on insurance premiums in 2012. As a result, farming families now have an extra 30 days to make payments without incurring interest penalties on unpaid premiums. August 1, the Secretary signed disaster designations for an additional 218 counties in 12 States as primary natural disaster areas due to damage and losses caused by drought and excessive heat. Source: <http://www.agprofessional.com/news/Vilsack-announces-new-drought-assistance-164602406.html>

Stinkbugs continue to plague soybeans across the U.S. Various stinkbug species are spreading quickly throughout the United States, Syngenta reported August 3. Growers as far apart as Louisiana and Nebraska say 25 to 35 stinkbugs are being reported per 100 sweeps, putting the health and yield of soybean plants in jeopardy. Soybean fields can quickly become the feeding ground for many different species of stinkbugs; the most common and damaging species include the green, the southern green, and the red-banded species, all of which continue to be found across the United States. In addition to the traditional species, a new stinkbug known as the brown marmorated stinkbug is being reported in various States across the country, and it is already a serious pest in vegetables and farm crops in the mid-Atlantic region. When stinkbugs invade a field, they remove fluids from soybean plants by feeding on the stems, foliage, blooms, and, most importantly, the developing pods and beans, causing significant damage to the quality of the soybeans and ultimately to the yield. Source: <http://www.agprofessional.com/news/Stinkbugs-continue-to-plague-soybeans-across-the-US-164623026.html>

Wisconsin firm recalls meat and poultry salad products due to potential *Listeria monocytogenes* contamination. Garden Fresh Foods, a Milwaukee establishment, recalled approximately 13,600 pounds of meat and poultry salad products. The salads contain diced onions that are the subject of a Food and Drug Administration recall by Gill Onions, due to possible contamination with *Listeria monocytogenes*, the U.S. Department of Agriculture's Food Safety and Inspection Service announced August 1. All the products were produced between July 10-16. The products were

UNCLASSIFIED

UNCLASSIFIED

distributed to retailers and institutions nationwide. Source:

[http://www.fsis.usda.gov/News & Events/Recall 051 2012 Release/index.asp](http://www.fsis.usda.gov/News%20&%20Events/Recall%20051%202012%20Release/index.asp)

Chopped onions with possible Listeria contamination trigger more recalls. Chopped yellow and white onions distributed by Gills Onions have triggered more recalls, as more food makers announced they were using the onions, which were first recalled July 18 for possible Listeria contamination, Food Safety News reported July 31. Garden Fresh Foods, Inc. recalled various ready-to-eat salads, slaw, salsa, bean, and dip products under various brands and code dates. Products were distributed in Arizona, California, Florida, Iowa, Illinois, Indiana, Massachusetts, Michigan, Minnesota, Missouri, Pennsylvania, Texas, and Wisconsin. Stop & Shop Supermarket Company LLC recalled its Calico Bean Salad sold in stores between July 18-26. Spartan Stores, Inc. recalled its Three Bean Salad and 10 ounce Broccoli Stir Fry sold between July 13-26. Publix Super Markets issued a recall of custom-made sub sandwiches that may have contained chopped onions connected to the recall, sold from July 7-26. Source:

<http://www.foodsafetynews.com/2012/07/chopped-onions-with-possible-listeria-contamination-trigger-more-recalls/>

USDA, EPA launch tool to better assess pathogen risk. The U.S. Department of Agriculture's (USDA) Food Safety and Inspection Service (FSIS) and the Environmental Protection Agency (EPA) announced July 31 that they have jointly developed a new tool to help "improve the quality of data collected and used to protect consumers from pathogen-related risks in food and water." The Microbial Risk Assessment (MRA) Guideline will help the government better assess the risks these pathogens pose to the public. An EPA Science Adviser said the project "contributes significantly" to improving the way federal agencies conduct microbial risk assessments and increases the transparency of the process so that stakeholders can better understand federal risk assessments. As USDA noted in their announcement, pathogens in food, water, and the environment can result in acute gastrointestinal-related illnesses and some can have long-term and permanent health effects as well as fatalities. Oftentimes, the source of pathogens is the same for water and food. The MRA Guideline outlines procedures that follow a "user-friendly, question-and-answer format that assists risk assessors in developing microbial risk assessments to meet agency-specific needs," according to FSIS.

Source: <http://www.foodsafetynews.com/2012/07/usda-epa-launch-tool-to-better-assess-pathogen-risks/>

Historic drought puts over half of U.S. counties in disaster zones, USDA says. More than half of all U.S. counties have been designated disaster zones, the Department of Agriculture (USDA) reported, blaming excessive heat and a devastating drought that has spread across the Corn Belt and contributed to rising food prices. The Agriculture Secretary August 1 declared disaster zone designations for an additional 218 counties in 12 States because of damage and losses caused by drought and excessive heat. The States are Arkansas, Georgia, Iowa, Illinois, Indiana, Kansas, Mississippi, Nebraska, Oklahoma, South Dakota, Tennessee, and Wyoming. Nearly three-quarters of the nation's cattle acreage is inside a region hit by drought, as is about two-thirds of the country's hay acreage, the agency reported. USDA researchers added that an average of 37 percent of the nation's soybeans the week of July 23 were ranked from very poor

UNCLASSIFIED

UNCLASSIFIED

to poor, the lowest quality recorded since a massive drought in 1988. Nearly half of America's corn crop was also rated very poor to poor, while 57 percent of its pastures and range land were similarly graded. Source: http://www.cnn.com/2012/08/01/us/us-usda-disaster-zones/index.html?hpt=hp_t1

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

EPA security breach exposes personal information of 8,000 people. A computer security breach at the Environmental Protection Agency (EPA) exposed the Social Security numbers and banking information of nearly 8,000 people, most of them current employees, the EPA confirmed August 1. The EPA told the Washington Business Journal in a statement that it notified 5,100 current employees and some 2,700 "other individuals" about a March security incident that exposed personal information on an EPA database. Those impacted were informed about the breach July 31, 4 months after it occurred. The EPA is offering free credit-monitoring services for 1 year to people affected by the breach. "EPA conducted a risk analysis, [which] indicates it is unlikely the personal financial information has been used," according to the EPA statement. "Vigilantly keeping data secure from increasingly sophisticated cyber threats is a top priority at EPA. The agency already added new safeguards in response to the incident." The agency's Office of the Inspector General confirmed an investigation is underway. Source: <http://www.bizjournals.com/washington/news/2012/08/02exposes-personal.html>

(Kansas) White powder sent in mail to KCK federal courthouse. The FBI is investigating after an envelope containing a "white powdery substance" was received in the mail July 30 at the Federal courthouse in Kansas City, Kansas. A hazardous materials crew was called to the building after a courthouse worker opened the envelope, according to the U.S. Marshals Service. There were no evacuations as a result of the incident, officials said. Source: <http://www.kansascity.com/2012/07/30/3732558/white-powder-sent-in-mail-to-kck.html>

Data breaches up 19 percent, GAO reports. Federal data breaches jumped 19 percent in 2011, the Government Accountability Office (GAO) said July 31. There were roughly 13,000 incidents reported by agencies in 2010 involving unauthorized disclosures of personally identifiable information — in 2011, that figure increased to 15,500, GAO's director of information security issues told the Senate subcommittee on government management oversight at a hearing. The subcommittee chairman questioned the head of the Federal Retirement Thrift Investment Board about a breach in 2011 that involved personally identifiable information of about 123,000 Thrift Savings Plan participants. Participants were not notified of the July 2011 breach until May 2012. The thrift board followed federal guidance in responding to the attack, but it lacked a notification plan for lack of funding, the board's executive director said. The agency will address data protection issues as part of its next record-keeping contract, to be awarded in fiscal 2013, he said. Source: <http://www.federaltimes.com/article/20120731/IT01/307310003/Data-breaches-up-19-percent-GAO-reports?odyssey=tab|topnews|text|FRONTPAGE>

UNCLASSIFIED

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Tools boast easy cracking of Microsoft crypto for businesses. A cryptography specialist released tools at the Def Con conference July 28 for easily cracking passwords in wireless and virtual private networks that use a popular encryption protocol based on an algorithm from Microsoft called MS-CHAPv2. The tools crack WPA2 (Wi-Fi Protected Access) and VPN passwords used by corporations and organizations running networks protected by the PPTP (Point-to-Point Tunneling Protocol), which uses MS-CHAPv2 for authentication. ChapCrack captures the MS-CHAPv2 handshakes, or SSL (Secure Sockets Layer) negotiation communications, and converts them to a token that can be submitted to CloudCracker. It takes less than a day for the service to return results in the form of another token that is plugged back into ChapCrack where the DES (Data Encryption Standard) keys are cracked. With that data, someone can see all of the information traveling across the Wi-Fi network, including sensitive corporate emails and passwords, and use passwords that were revealed to log in to corporate networks. The tools are designed for penetration testers and network auditors to use to check the security of their WPA2 protected networks and VPNs, but they could also be used by people who want to steal data and get unauthorized access to networks. Source: http://news.cnet.com/8301-1009_3-57481855-83/tools-boast-easy-cracking-of-microsoft-crypto-for-businesses/

New Morto worm variant emerges with file infection capability. A new variant of the Morto worm added a file infection capability to the malware's arsenal of weapons, warned a Microsoft researcher. The original Morto worm was able to compromise remote desktop protocol (RDP) connections by exploiting weak administrator passwords, but the new strain has added file infection capability to its repertoire, noted the researcher with the Microsoft Malware Protection Center. He explained that the new Morto variant "infects .EXE files found on fixed and removable drives as well as on default RDP and Administrative shares, but avoids infecting files that contain strings like 'windows', 'wintt', 'qq', 'Outlook', 'System Volume Information' or 'RECYCLER' in their path. Morto also leaves an infection marker, 'PPIF' in infected files." Source: <http://www.infosecurity-magazine.com/view/27277/>

Hiding SAP attacks in plain sight. As some of the biggest processors of regulated data in any large organization, business-critical applications like enterprise resource planning (ERP) applications from SAP are well within the purview of compliance auditors and malicious attackers. Many organizations believe that if these systems are set behind firewalls, they are safely segmented enough to not require further hardening. However, as one researcher demonstrated at Black Hat the week of July 23, business-critical application servers never process data as an island, and in those connections there are opportunities for attack by hiding malicious packets within admissible ones. Called server-side request forgery (SSRF), the attack technique highlighted by the head of Russian firm ERPScan makes it possible to execute a multi-chained attack on SAP applications that can be executed from the Internet while bypassing firewalls, IDS systems, and internal SAP security configurations. Source: <http://www.darkreading.com/database-security/167901020/security/news/240004610/>

NATIONAL MONUMENTS AND ICONS

(Idaho) Halstead Fire nears 10,000 acres. A lightning-caused wildfire northwest of Stanley, Idaho, jumped from 50 to nearly 10,000 acres over the course of a few days, the U.S. Forest Service reported August 2. The Halstead Fire, located near Highway 21, started July 27 when a lightning strike ignited a ridge between Beaver Creek and Marsh Creek, a tributary of the Middle Fork of the Salmon River. Fire crews were removed from the scene over the weekend of July 28 due to the extremely hot and active nature of the fire, but returned to work July 30. A spokeswoman for the Salmon-Challis National Forest stated in a press release August 2 that the fire reached 9,626 acres. The scout camp, as well as national forest campgrounds at Beaver Creek, Beaver Creek Spur, Lola Creek, Lola Camp Spur A, Marsh Creek Transfer, and Josephus Lake were closed. All access to the Cape Horn, Seafoam Bubble, and the Pinyon Peak roads were closed. Trails in the area — including the Halstead Trail, the Roughneck Trail, the Marsh Creek Trail, and the Middle Fork Trail from the trailhead to the junction with Fall Creek Trail were closed. Source: <http://www.mtexpress.com/index2.php?ID=2005143236>

POSTAL AND SHIPPING

Nothing Significant to Report

PUBLIC HEALTH

(Indiana) Investigation into health facility break-in continues. A safe containing personal and financial information belonging to patients of Kindred Transitional Care and Rehabilitation in Sellersburg, Indiana, was stolen during a break-in at the facility between June 1 and June 4, according to a statement released by Kindred officials. The safe contained tapes listing patients' information, including Social Security numbers, diagnosis, dates of birth, home addresses, insurance numbers, dates of care, medications provided, and bank account numbers. A Clark County Sheriff's Department spokesperson said it did not appear there was any forced entry made into the office where the safe was located, but drawers in the room did appear to be have been forcefully opened. He said deputies monitored the compromised names to see if the suspect or suspects would attempt to steal any of patients identities, but it appeared no attempts were made. Source: <http://newsandtribune.com/local/x1402344936/Investigation-into-health-facility-break-in-continues>

(Michigan) Michigan hospitals linked to hepatitis-C investigation. Michigan State health officials said July 30, a traveling medical technician accused of causing a hepatitis C outbreak in New Hampshire worked in at least six Michigan facilities from 2003 to 2007. Officials said patients who underwent procedures between 2005 and 2007 at the four remaining hospitals — Harper, Sinai Grace, University of Michigan Hospital, or Oakwood Annapolis — should probably be tested for possible exposure. The Michigan Department of Community Health said its "investigation has not uncovered evidence that the individual was infected with hepatitis C while employed at any Michigan facility," and a negative test result at one Michigan hospital

UNCLASSIFIED

allowed them to exclude two hospitals from further examination. Source:

<http://detroit.cbslocal.com/2012/07/30/michigan-hospitals-linked-to-hepatitis-c-investigation/>

TRANSPORTATION

Nothing Significant to Report

WATER AND DAMS

(Oregon) State: Toxic algae in nearby reservoir. A health advisory was issued July 31 due to high levels of blue-green algae in Dorena Reservoir, 6 miles east of Cottage Grove in Lane County, Oregon. Water monitoring confirmed the presence of blue-green algae that can produce toxins. Swallowing or inhaling water droplets should be avoided, as well as skin contact with water. Drinking water from the reservoir is especially dangerous and Oregon Public Health officials advised campers and other reservoir visitors that toxins cannot be removed by boiling, filtering, or treating the water with camping-style filters. People who draw in-home water directly from Dorena Reservoir were advised to use an alternative water source because private treatment systems are not proven effective in removing algae toxins. Oregon health officials also recommended that people who choose to eat fish from waters where algae blooms are present should remove all fat, skin, and organs before cooking because toxins are more likely to collect in these tissues. The public will be advised when the concern no longer exists. Source: <http://www.kval.com/news/local/State-Toxic-algae-in-nearby-reservoir-164514036.html>

HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **North Dakota State and Local Intelligence Center: 866-885-8295 (IN ND ONLY);** Email: ndslic@nd.gov; Fax: 701-328-8175 **State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.**

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168

UNCLASSIFIED